The Armenian Center
for National and International Studies

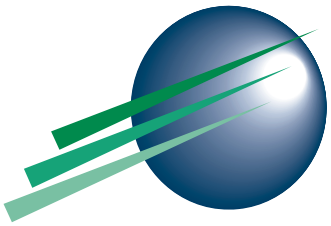
Ռազմավարական եւ ազգային հետազոտությունների
հայկական կենտրոն

Армянский центр стратегических и
национальных исследований

КАРЕН МАТЕВОСЯН
кандидат технических наук

Основные задачи обеспечения живучести и информационной безопасности национальной сети связи Армении

17 декабря 2009 г.
Ереван



Армянский центр стратегических и национальных исследований

Основные задачи обеспечения живучести и информационной безопасности национальной сети связи Армении

Карен Матевосян
Кандидат технических наук

Рассматриваются методы и технологии обеспечения живучести сетей систем и инфраструктур в условиях внешних воздействий, а также информационная безопасность компьютерных сетей и систем. Сформулированы основные задачи, которыми следует руководствоваться для формирования политики страны при построении надежной и живучей национальной сети.

Определения:
Живучесть сети *(survivability):*
– это способность сохранять связность и выполнять установленные функции, в допустимых пределах снижения их качества, при воздействии разных дестабилизирующих факторов (при отказе отдельных ее узлов или участков сети);
– это способность к адаптации, самоорганизации в непредвиденных аварийных ситуациях, путем реконфигурации структуры и коррекции режима функционирования.

Живучесть национальной сети связи:
– это комплекс мероприятий по защите информационной инфраструктуры страны в целом, включающий обеспечение надежного функционирования,

защиту и гарантированную доставку информации, эффективное управление, а также физические методы и средства защиты сети.

***Национальная сеть связи страны**:*
– это физическая основа всей совокупности информационных систем управления государства.

Развитые информационные и телекоммуникационные технологии - важная составляющая жизнедеятельности страны. Сегодня информационные системы управления охватывают, практически, все сферы государственного и хозяйственного управления Армении, включая экономику,
органы государственной власти,
финансовую деятельность,
национальную безопасность,
социальную и духовную жизнь общества и другие сферы жизнедеятельности страны.

Многие информационные системы управления представляют собой сложный, крупномасштабный территориально-распределенный комплекс, состоящий из десятков серверов и сотен рабочих станций, опирающийся на республиканские сети и использующий трансконтинентальные телекоммуникационные магистрали.

Все эти действующие системы управления образуют информационную инфраструктуру страны, а используемые ими каналы и сети связи, независимо от их принадлежности, составляют, в совокупности, национальную сеть (НС) связи.

Особенности национальной сети связи Армении

Национальная сеть связи Армении, фактически, более чем на 90% строится на базе магистральных каналов и сетей связи общего пользования частных, иностранных операторов связи, предоставляемых на арендной основе. При этом интересы операторов связи и государства в отношении к НС не во всем совпадают.

Все применяемые на сетях аппаратные средства, операционные системы, и большинство программных продуктов, используемых на сетях связи страны - зарубежного производства. Более того, большая разнотипность используемых технических средств и крайне недостаточный уровень их сертификации, наличие на сети физически и морально устаревшего оборудования, а также применение, во многих случаях, не обновляемых, «пиратских» версий операционных систем

существенно обостряют проблему информационной безопасности и создают неустойчивость в работе сети и уязвимость к различного рода воздействиям, а в некоторых случаях, способствуют и утечке информации.

Пользуясь информационными и транспортными услугами сети Интернет и других глобальных телекоммуникационных сетей, Армения стала частью мирового информационного пространства, которое содержит в себе немало угроз криминального и террористического характера национальным интересам страны. К тому же, Армения окружена далеко не дружественными странами, что чревато, потенциально, угрозой информационной безопасности страны. Можно не сомневаться, что разведывательные службы этих государств (и не только этих) осуществляют сбор политической, экономической, военной и прочей конфиденциальной информации о нашей стране, используя разные источники, в том числе и сетевую информацию. И, безусловно, эти страны вынашивают против Армении планы информационной войны, предусматривающие нарушение работы информационных и телекоммуникационных систем. Информационное оружие сегодня уже не фантастика, а реальность, и оно, по своей результативности, сопоставимо с оружием массового поражения.

Предпринимаемые частные меры по защите отдельных ведомственных систем управления не способны решить проблему информационной безопасности страны в целом, в силу ряда причин, основные из которых - недостаточность профессионального опыта проектирования и строительства таких систем и ограниченность финансовых возможностей на приобретение необходимых программных и технических средств. Частными операторами сетей проблема информационной безопасности решается, в первую очередь, в рамках своих, корпоративных интересов.

Приведенные особенности НС обуславливают ее весьма низкую защищенность, что не может удовлетворять национальным интересам обеспечения безопасности информационных и телекоммуникационных систем, как действующих, так и создаваемых в нашей стране. Информационная безопасность, наряду с военной, экономической, экологической является важнейшей составляющей национальной безопасности. Поэтому, исходя из интересов безопасности страны, в целях создания единого защищенного информационного пространства, необходимо обеспечить национальной сети высокую надежность и живучесть для защиты информационных ресурсов, как от внешних и внутренних угроз, так и в случаях непредвиденных природных и техногенных катастроф.

Для этого должны быть решены такие задачи как:

- **обеспечение живучести НС;**

- **повышение надежности используемых в НС технических средств;**
- **обеспечение гарантированной целостности и конфиденциальности передаваемой и хранимой в НС информации;**
- **построение эффективной системы сетевого мониторинга и управления функционированием НС.**

Наряду с этим, потребуется принятие ряда организационных, правовых и других решений.

Создание в стране собственной национальной сети с высокой эксплуатационной надежностью и живучестью потребует значительных материальных затрат. Более того, эта задача усложняется необходимостью внедрения новых технологий и услуг, а также замены морально и физически устаревающего оборудования. Для Армении, в ближайшие годы, такая задача непосильна. Ее решение должно быть осуществлено на базе действующих в стране сетей и наименее затратным способом, не нарушая, при этом, прав собственников сетей и с их участием.

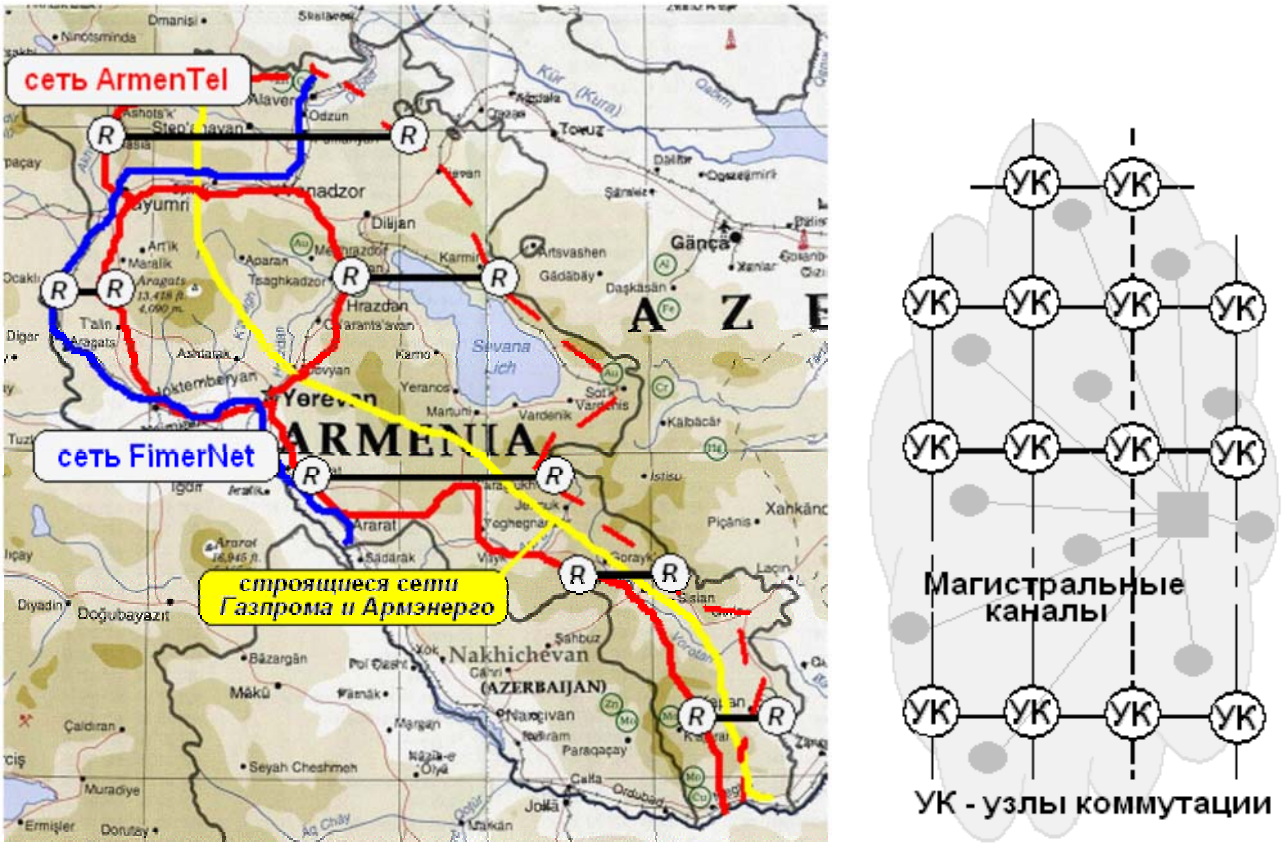
Основной подход должен состоять в осуществлении взаимоувязки существующих и создаваемых сетей между собой, максимально используя применяемые на сетях аппаратные и программные средства, так, чтобы обеспечить связанность, высокую готовность, бесперебойность работы и, в конечном итоге, живучесть национальной сети. Уменьшению затрат будет способствовать также аудит действующих систем управления с целью выявления уязвимых, подверженных рискам узлов и сегментов сети, с учетом степени важности и ответственности решаемых ими задач.

При этом если обеспечение надежной, бесперебойной работы сети и гарантированных услуг входит в круг интересов собственников сетей, то планирование работ по обеспечению живучести национальной сети и информационной безопасности являются ответственной задачей государства.

Обеспечение живучести НС

Именно живучесть может рассматриваться как наиболее объективный показатель, позволяющий наилучшим образом оценить структурную и функциональную надежность сети. Критерием оценки живучести является способность сети к реконфигурации и сохранение, в условиях деградации, в заданных пределах, показателей таких сетевых ресурсов, как производительность (или пропускная способность) сети, время реакции системы, показатели качества обслуживания (Quality of Service, QoS), оговоренные в соглашении об уровне обслуживаня (Service Level Agreement, SLA) и др.

При решении проблемы живучести, в первую очередь, должна быть обеспечена надежность функционирования и живучесть магистральных связей в стране. В Армении действуют и создаются новые скоростные магистральные оптические каналы связи, пронизывающие республику с севера на юг. Высокая степень живучести магистральной сети может быть обеспечена организацией горизонтальных связей (с запада на восток) между проложенными магистралями, образуя многоканальную ячеистую сеть.



Магистральная ячеистая сеть

В свою очередь, привязка региональных и местных сетей к такой магистральной сети, с необходимой степенью резервирования узлов и каналов связи, обеспечит им высокий уровень живучести.

Дополнительно, существенное повышение живучести НС может быть достигнуто за счет использования альтернативных видов связи, таких как спутниковая связь и радиосвязь по технологии WIMAX для резервирования кабельной магистральной сети, и на местном уровне - радиосвязь по технологии WiFi и

сотовую связь. Использование этих видов связи и их топология в составе НС должны решаться в ходе проектирования.

Безусловно, что подобная организация магистральной и региональной связи отвечает также интересам операторов сетей, создавая резервные обходы в критических ситуациях, однако реализация такого решения в комплексе может быть осуществлена лишь при определяющей и регулирующей роли государства.

Повышение надежности технических средств НС

Основным методом обеспечения надежности, является избыточность. Избыточность подразумевает структурное и функциональное резервирование оборудования критически важных коммутационных устройств узлов сети и каналов связи, что позволит поддерживать в автоматическом режиме их работоспособность при отказах.

Например, в случае, когда в составе узла сети резервные элементы функционируют параллельно с основными (так называемое «горячее» резервирование), надежность такой системы возрастает более чем на порядок, по сравнению с надежностью каждого из ее элементов.

В свою очередь, резервирование каналов, связывающих пользовательское оборудование с узлами магистральной сети, с их географическим разнесением, по принципу «исключение в структуре сети единой точки отказа», придаст высокую отказоустойчивость сети связи информационной системы управления.

Критерием оценки надежности системы является **готовность**, что подразумевает гарантированное обеспечение доступности информации или ее передачи в заданном интервале времени в процессе эксплуатации. Готовность характеризуется коэффициентом ($\mathbf{K_г}$), определяемым соотношением между периодами времени безотказной работы ($\mathbf{t_0}$) и временем простоя системы ($\mathbf{t_{пр}}$).

$$\mathbf{K_г = t_0 / (t_0 + t_{пр})}$$

При дублировании оборудования, в режиме горячего резервирования, может быть достигнут $\mathbf{K_г}$ = 0.999 – 0,9995, что соответствует суммарному времени простоя отказавшего узла или участка сети в течение, например, одного года, около 9 часов и 4,4 часа соответственно. При наличии обходов на сети, такое время простоя практически не скажется на качестве работы сети.
Основной недостаток такого метода обеспечения надежности – повышенные материальные затраты, в связи с чем, решение о резервировании должно приниматься в зависимости от степени ответственности конкретной системы. Сокращению затрат будет способствовать резервирование на основе анализа уязвимости сети и оценки рисков отказов.

Обеспечение целостности и сохранности обрабатываемой в НС информации

Задача – обеспечить гарантированную защиту и конфиденциальность обрабатываемой в НС информации от внешних и внутренних угроз.

Эффективным средством защиты передаваемой информации является технология виртуальных частных сетей, технология VPN (Virtual Private Network). С помощью этой технологии строится надежно защищенная виртуальная сеть внутри любой сети общего пользования (сети с технологией IP, Frame Relay, ATM, Internet), образуя в них "скрытые", защищенные от посторонних, каналы связи.

Безопасность информации, обрабатываемой в таких сетях, обеспечивается использованием эффективных криптографических методов и средств защиты. Технология VPN позволяет объединить в единую защищенную виртуальную сеть локальные сети с произвольным числом рабочих станций, удаленных и мобильных пользователей, создавать защищенные мультисервисные корпоративные сети и организовать межсетевое взаимодействие с разными виртуальными сетями.

Использование технологии VPN в составе информационных систем управления создаст достаточный уровень безопасности телекоммуникационной среды страны и, соответственно, безопасность и достоверность информационных ресурсов НС, даже при использовании общедоступной сети Интернет в качестве транспортной среды. В сетях VPN осуществляется автоматизированный контроль и управление связями, правами и полномочиями всех объектов виртуальной среды.

Важной особенностью применения технологии VPN является обеспечение защиты информационных ресурсов сети без замены, в большинстве случаев, используемого на сети оборудования.

Безопасность, целостность и конфиденциальность информации в сети VPN обеспечивается системой межсетевого и персонального шифрования передаваемого трафика, идентификацией (аутентификацией) клиентов и электронной цифровой подписью, подтверждающей юридическую верность передаваемых через сеть документов, а также фильтрацией сообщений и пакетов.

Шифрование данных является одним из основных механизмов защиты, гарантирующим целостность и конфиденциальность информации. Степень защиты определяется алгоритмом шифрования и длиной используемого ключа шифрования. Достаточно высокий уровень защиты обеспечивается при использовании ключей, длиной более 128 бит. К примеру, ключ широко используемого алгоритма AES (Advanced Encryption Standard) содержит в себе 128 разрядов, но стандарт может поддерживать и более длинные ключи в 192 и

256 разрядов. Ключи такого размера обеспечивают высокую гарантию от взлома закрытой информации.

В сетях VPN предусмотрены также механизмы проверки целостности и подлинности передаваемых данных, что гарантирует получение информации именно в том виде, в котором ее отправляли, без потерь и подмен.

Наряду с криптографическими средствами, эффективную защиту технических и информационных ресурсов VPN-сети от попыток проникновения нарушителей в сеть, как извне, так и изнутри, обеспечит применение распределенной системы межсетевых и персональных сетевых защитных экранов (firewall).

Мониторинг и управление функционированием НС

Задача - создание централизованной системы сетевого мониторинга и управления функционированием НС, обеспечивающей контроль и диагностирование сети, оперативное обнаружение в реальном времени нарушений, и взаимодействующей с распределенными службами мониторинга и управления сетей общего пользования и информационных систем.

Необходимым условием организации эффективной системы управления национальной сетью является построение ее с учетом иерархической трехуровневой архитектуры сети.

Трехуровневая архитектура сети

Верхний или магистральный уровень образуется главными узлами. Средний - состоит из региональных сетей, обслуживающих ограниченную территорию (район, область). Нижний уровень составляют сети доступа, к которым подключаются пользователи.

Узлы среднего уровня могут быть соединены с несколькими узлами верхнего уровня. Так же с несколькими узлами среднего уровня и могут быть связаны сети доступа.

Такой подход позволяет осуществлять независимое, на каждом уровне, управление сетью, а также развивать и реконструировать каждый уровень независимо друг от друга, и, при необходимости, производить реконфигурацию сети. И, кроме того, все организации, имеющие распределенную информационную систему, смогут осуществлять взаимодействие собственной системы мониторинга с уровневыми системами управления национальной сетью, что будет способствовать повышению надежности функционирования этих систем.

Заключение

Реализация рассмотренных методов обеспечит надежность функционирования, информационную безопасность и живучесть НС в масштабах страны. Однако такая крайне важная для Армении проблема не может быть решена только одними рыночными механизмами.
Положительного результата можно достигнуть, в течение 3-х – 4-х лет, при активной роли государства в части координации и регулирования взаимоотношений и взаимодействий всех участников этого направления. При этом формирование национальной сети связи должно стать целевой программой государства.

Литература

1. Додонов А.Г., Кузнецова М.Г., Горбачик Е.С. Введение в теорию живучести вычислительных систем. – Киев, Наукова думка, 1990.
2. Богатырев В.А. Отказоустойчивость и сохранение эффективности функционирования многомагистральных распределенных вычислительных систем. Информационные технологии, 1999, №9, С.П.
3. Богатырев В.А. Надежность отказоустойчивых вычислительных систем реального времени, компонуемых из многофункциональных модулей. Информационные технологии, 2000, №10. С.П.
4. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. В 2-х кн. Книга 1. М. Энергоатомиздат, 1994. . 400 с.
5. Устинов Г.Н. Основы информационной безопасности систем и сетей передачи данных. Учебное пособие. Серия «Безопасность». М., СИНТЕГ, 2000. 248с.
6. Охтилев М.Ю., Соколов Б.В., Юсупов Р.М. Интеллектуальные технологии мониторинга и управления структурной динамикой сложных технических объектов. - М.: Наука, 2006.